BLINC: Inclusive Blockchain for Digital Citizenships

BLINC: Inclusive Blockchain for Digital Citizenships

Fadi Barbara, Guido Boella
Alex Cordero, Claudio Schifanella
Department of Computer Science
University of Turin, Italy
{name.surname}@unito.it

Serena Ambrosini, Alberto Ferrini
CS InIT
Consoft Group spa
Turin, Italy
{name.surname}@consoft.it

Luca Lattore, Francesco Zucaro
Wave Infomatica
Turin, Italy
{name.surname}@waveinformatica.com

Mario Pissardo, David Manfrin
CSI Piemonte
Turin, Italy
{name.surname}@csi.it

***Abstract*—We present BLINC, an Italian regional project funded by European Union via the European Regional Development Fund. BLINC proposes a completely decentralized solution to manage documents in a privacy preserving manner using the Ethereum pubblic blockchain for notarization and access control lists combined with IPFS for decentralize storage. Thanks to the mobile applications we developed, the users can create a web of trust which can help the integration process for migrants.**

I. Introduction

The BLINC project aims to test and verify the effectiveness of blockchain technologies for the management of documents, certificates and information, in order to build a web of trust for migrants [1]. The web of trust aims at bridging the information gap that hinders immigrants inclusion processes, without leading to social stigma or discrimination in the right to privacy [2]. The framework proposed by the BLINC project is a virtual document wallet, that can store self-generated certificates (e.g. starting from paper documents or by declaration) next to official documents, generated by private and public services. The document wallet is mainly designed for mobile devices and at the same time, accessible from any other networked device. It is based on an easy-to-use interface, designed for any level of skill in managing digital devices.

A leading property of the BLINC system is the granular management of privacy, not intended as a discriminating file, but as an opportunity to collect traces that will allow immigrants to accelerate their social inclusion.

II. The Application

A. Logic architecture and elements

BLINC project main outcome is represented by a native mobile App, built on top of the Ethereum network, and supports the following use cases:

- Provides a digital document folder, in which each documents privacy is under control of the final user, even if shared with others (granular privacy)
- Permits secure and private sharing of documents between trusted users.
- Endorses personal declarations between trusted and verified users

In this scenario, document notarization, privacy, security ACL, endorsement and sharing between users are implemented by Ethereum Smart Contracts, that run on top of an Ethereum Network. Document storage is provided by a Decentralized IPFS network. A back-office web application is provided, to validate user registration inside BLINC Network, by verified associations that are interested in enabling their real users to enter the BLINC network of trust.

B. Documents and declarations

BLINC wallets are divided in two sections: one for *documents*, another for *declarations*. Documents are digital representations of real official documents, released by recognized authorities (e.g. VISA, Personal ID, Driving Licence). These documents can be verified by the associated public services offices, inside the BLINC network. Declarations are self-produced documents, that state some mutual interaction between users (e.g. a recommendation letter from an employer), representing a value of trust or self-certification. Declarations can be shared and endorsed by users that receive the corresponding document, to give a self-certification to the value of the content inside the declaration. Sharing documents and endorsing declarations are registered transaction on the Ethereum blockchain, so that there is no need for a third-party verification of the status of the data inside the user wallets. The decentralized nature of the blockchain provides a public access peer-to-peer verification process, so that the status of the blockchain represents the web of trust, as the main goal of the project.

III. Document security and privacy

Data security and privacy is granted by the users identities themselves. Any user is provided with a pair of cryptographic keys, that is used during the encryption of the documents.

BLINC project is funded by POR-FESR 2014/2020- Regione Piemonte

For reasons related to the file size of the encrypted documents, the document itself is encrypted using a symmetric encryption scheme. The symmetric key is then encrypted using the owners public key, following an asymmetric encryption scheme. Therefore there will be only encrypted data on the decentralized storage, namely the encrypted document and the encrypted symmetric key. If the owner A wants to share the encrypted document with a user B, the symmetric key will be decrypted and re-encrypted using the public key of user B. We use a smart contract [3] which implements an access control list in case A needs to revoke the sharing. This way unauthorised access is prevented even to users who already own the symmetric key.

IV. Granular privacy and smart contracts

The main goal of this project is to allow users to build a network of trust while keeping complete control over the status of the documents they store in their personal wallet. The owner of a document has complete power over the possible states of it: he is the only one in charge for granting and revoking sharing of his documents around the BLINC network.

The Ethereum Blockchain can provide a decentralized layer of control about the status of the network, between users and documents, so that there is no central authority to maintain and validate this status. Any user inside the network can build his own network of trust, letting it been validated by the status of the blockchain. At the same time, anyone inside the network can inspect and verify the history and the status of the network.

A. Signup Registry

The status of any single document and its history is controlled by a Signup Registry Smart Contract: it is responsible of registering new documents, maintaining the list of users that the owner has shared his documents with and the list of endorsements a declaration has received inside the network.

When a new document is stored in a users wallet, after been encrypted and secured, the registry create a t-uple of data which is used to uniquely identify the document in the decentralized storage.

B. Document ACL

Since the access to any document has to be regulated by the user, a smart contract that builds an ACL matrix between each document and the users that can have access to it.

C. Sharing Documents

The process of sharing a new document involves two aspects. First, a document owner has to be contacted from a user who wants to be in his trusted network. After that, the document owner has to directly enable the sharing of a document to one or more contacts inside his network.

To be included in the owner's network, a user must send to the owner an URL which is a representation of the user's public key. adding this key to the list of trusted contacts makes the document owner able to share documents with him. As stated in Section III, the user public key is used to encrypt the symmetric key used to secure the original document data. This information is added inside the ACL row, and corresponds to the user right to access the document: this user can decrypt the symmetric key with his own private key and access the encrypted document decrypting it with the symmetric key.

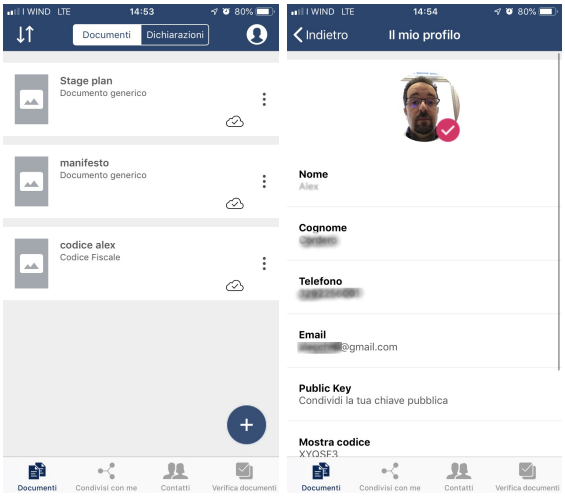

Fig. 1: The BLINC iOS app

D. Endorse declaration

Endorsing declarations is a simple notarization process, driven by the signup registry smart contract. A user can navigate the list of declarations shared with him and add an endorsement, that grants his level of trust about the validity of the declaration, e.g. a landlord can endorse an immigrant about a well-conducted rental contract shared to him by the immigrant itself. A third-party association, such as a rental public or private service, can verify this information without any need of central validation: the endorsement has been registered as a blockchain transaction, therefore his state is immutable and accessible to anyone. This functionality has been added to incentivize the sharing of chosen information between trusted parties and increase the value of decentralized trust inside the network of BLINC users.

V. Conclusions

We described a decentralized framework to securely store and share digital documents by using blockchain and smart contracts for document notarization and ACLs, and a decentralized file system as storage. Currently, we are working together with ACLI Torino in the evaluation of how BLINC application, available both as Android and iOS app, can help migrants during the integration process.

References

[1] Matthew Richardson M., Rakesh Agrawal R. and Pedro Domingos P., "Trust Management for the Semantic Web" 2003
[2] Slobogin, C. "Public privacy: camera surveillance of public places and the right to anonymity." 2002.
[3] Bartoletti, M., Pompianu, L. "An empirical analysis of smart contracts: platforms, applications, and design patterns".